UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/461,010	12/15/1999	PIERRE CALVEZ	6313	3226

7590 11/12/2003

EDWARD J KONDRACKI
MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 221023833

EXAMINER	
AKPATI, ODAICHE T	
ART UNIT	PAPER NUMBER
2131	11

DATE MAILED: 11/12/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/461,010	Applicant(s) CALVEZ ET AL.	
	Examiner Tracey Akpati	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____ .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)□ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20-52* is/are rejected.

7)☒ Claim(s) *20-52* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☒ The proposed drawing correction filed on *15 December 1999* is: a)☒ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) □ Interview Summary (PTO-413) Paper No(s). _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: .

DETAILED ACTION

Claim Objections

Claims 20-52 are objected to because of the following informalities: Figure numbers are not supposed to be used within the claim language. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 47, 48, 49, 50 and 52 are rejected under 35 U.S.C. 102(e) as being anticipated by Ishii (5768389).

With respect to Claim 47 the limitation "A computer system (1) for creating and managing pairs of asymmetrical cryptographic keys and certificates associated with the pairs of keys, the pairs of keys and the certificates being intended for subjects managed by said system, comprising a key generating center (8) for creating at least one pair of keys at the request of the local registration authority (5) with which the key generating center communicates; at least one certification authority (12) to which the system has access for creating a certificate at the request of the local registration authority (5) and means for automating the creation and/or certification of at least one pair of keys for each subject managed by the system (1)" is met by Ishii on column 8, lines 8-24 and Fig. 2.

With respect to Claim 48, the limitation "a central management service (3) for creating, updating and consulting objects and subjects managed by said system a local registration authority (5) for handling the creation and/or the certification of keys intended for the objects and the subjects a central security base (7) containing the subjects and the objects managed by the system with which the local registration authority communicates a key generating center (8) for creating at least one pair of keys at the request of the local registration authority (5) with which the key generating center communicates; and at least one certification authority (12) to which the system has access for creating a certificate at the request of the local registration authority" is met by Ishii on Figure 5.

With respect to Claims 49 and 50, the limitation "a wake up mechanism for periodically waking up the local registration authority" is obvious to one of ordinary skill in the art to incorporate into the invention because a wake up mechanism would be necessary for continuous generation and replacement of old keys and certificates, hence yielding a safer key management system.

With respect to Claim 52, the limitation "a computer system (1) for creating symmetrical cryptographic keys, for managing subjects by said system, characterized in that it comprises a key generating center (8) for creating at least one pair of keys at the request of the local registration authority (5) with which the key generating center communicates; at least one certification authority (12) to which the system has access for creating a certificate at the request of the local registration authority (5) and means for automating the creation of at least one key for each subject managed by the system(1)" is met by Ishii on column 1, lines 26-29, column 11, lines 50-67 and column 12, lines 1-46.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 20-22, 26-35, 45,46 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (5768389) in view of Van Oorschot (6370249B1).

With regards to Claim 20, the limitation "creating at least one first individual request for creating and certifying a pair of asymmetric keys for said subject" is met by Ishii on column 11, lines 31-33 and 63-67.

The limitation "transmitting a key generation request corresponding to said first individual creation ε certification request to a key generating center (8), which issues a pair of asymmetric keys in accordance with said key generation request" is met by Ishii on column 11, lines 20-62.

The limitation "creating at least one second individual request for certifying the public key created f said subject" is met by Ishii on column 11, lines 63-67.

The limitation "transmitting a certification authority request corresponding to said second individua certification request to a certification authority (12), which issues a certificate in accordance with said requ is met by Ishii on column 12 on lines 12-16 and 42-46. Ishii however does not disclose searching a storage means for the subject that needs the asymmetric keys. This is however disclosed by Van Oorschot.

The limitation "searching in storage means (7) for at least one subject for which a pair of asymmetric keys and an associated certificate must be created" is met by Van Oorshot on column 3, lines 24-33.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the system of Ishii because retrieval of the subject from a list that may have already been authenticated is more secure than relying on the user to prove that they are who they say they are.

With respect to Claim 21, Ishii discloses all the limitation except the criteria or circumstances for which the creation of a pair of keys is necessary.

The limitation "creating a pair of keys must be created for a given subject when said subject lacks a pair of keys and a corresponding first individual creation and certification request, or when a pair of keys has been requested for said subject, or when the certificate of a pair of keys for said subject intended for an identical use has been revoked and a new pair of keys has been requested" is met by Van Oorschot on column 4, lines 37-49.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorshot to the system of Ishii because it is a natural step to create a pair of keys in the event of the former set of keys being revoked or a set of new keys being requested.

With respect to Claim 22, Ishii meets all the limitation except that of periodical generation of keys and certificates.

The limitation "executing said process periodically" is met by Van Oorschot on column 3, lines 14-19.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the system of Ishii because a periodical generation of new keys provides a more secure computer system as shown by Menezes on page 183, section 8.10. Menezes states that the longer a key is used, the greater chance it will be compromised and the greater the loss.

With respect to Claims 26-28, Ishii meets all the limitation except that of searching for the subject that required the new keys.

The limitation "searching in each of the multiple creation and certification requests of the system for all of the subjects in a condition such that a pair of keys must be created" is met by Van Oorschot on column 4, lines 37-47.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot to the system of Ishii so as to find the correct and authorized recipient of the keys, and hence prevent the sending of keys to an unauthorized individual.

With respect to Claim 29, the limitation "creating at least one individual certification request for certifying a public key" is met by Ishii on column 11, lines 63-67.

The limitation "transmitting a certification authority request corresponding to said individual certification request to a certification authority (12), which issues a certificate in accordance with said request" is met by Ishii on column 12, lines 12-16 and 42-45. Ishii however does not disclose searching the storage means for a pair of asymmetric keys. This is disclosed by Van Oorschot.

The limitation "searching in storage means (7) for at least one pair of asymmetric keys for the public key for which a certificate must be created" is met by Van Oorschot on column 3, lines 24-37.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the system of Ishii because referring back to an already secure storage means for the necessary keys allows the system to save the time it would have used to request and authenticate the sender of the keys from a remote area.

With respect to Claim 30, the limitation "certificate for a given subject when said subject lacks a certificate and an individual certification request, or when a certificate has been requested for said subject, or when the certificate of a pair of keys for said subject expires, or when the certificate of a pair of keys has been revoked" is met by Ishii on column 12, lines 17-20.

With respect to Claim 31 and 32, Ishii meets all the limitation except that of periodically executing the process.

The limitation "executing said process periodically" is met by Van Oorschot on column 3, lines 14-19.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the system of Ishii because a periodical generation of new keys provides a more secure computer system as shown by Menezes on page 183, section 8.10. Menezes states that the longer a key is used, the greater chance it will be compromised and the greater the loss.

With respect to Claims 33-35, the limitation "creating the certificate for a given subject when the certificate expires during this period" is met by Ishii on column 12, lines 17-50.

With respect to Claim 45, the limitation "consists of performing the encoding of one or more extensions in accordance with one or more given rules and of entering the encoded extension or extensions into the individual certification request during the creation of said individual certification request" is met by Ishii on column 11, lines 63-67 and column 12, lines 1-3.

With respect to Claim 46, the limitation "changing the value of an attribute contained in each of the individual first and second requests to indicate status of the process" is met by Ishii on column 1, lines 51-63.

With respect to Claim 51, the limitation "creating at least one individual request for creating a symmetric key for said subject" is met by Ishii on column 11, lines 20-21 and 31-33.

The limitation "transmitting a key generating request corresponding to said individual creation request to a key generating center (8)" is met by Ishii on column 11, lines 31-33.

The limitation "issuing by said key generating center a symmetric key in accordance with said transmitted key generating request" is met by Ishii on column 11, lines 35-62.

The limitation "searching in storage means (7) for at least one subject for which a symmetric key must be created" is partly met by Van Oorschot on column 3,lines 24-33. Van Oorschot does not disclose a symmetric key system. This is however disclosed by Ishii on column 1, lines 26-29.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the system of Ishii as to achieve high speed processing as disclosed by Ishii within the same excerpt from the reference.

Claims 23-25, 36-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (5768389) in view of Van Oorschot (6370249B1) in further view of Aziz (6330671 B1).

With respect to Claim 23-25, Ishii meets all the limitation except that described below.

The limitation "wherein each individual first and second request is created from corresponding multiple creation and certification requests stored in the storage means…" is met by Van Oorschot on column 3, lines 20-38.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the system of Ishii so allow for the secure creation of keys for the required authorized individual.

The combination of Ishii and Van Oorschot however does not disclose a set of subjects belonging to a preset list. This is however disclosed by Aziz.

The limitation "…relative to a set of subjects belonging to a preset list or to a set of subjects defined by predetermined criteria, as well as to model pairs of keys and associated model certificates for the set in question" is met by Aziz on column 4, lines 1-21.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Aziz within the combination of Ishii and Van Oorschot so as to allow for the retrieval of an already authorized list of subjects and hence lessens the likelihood for the creation and transmission of keys to an unauthorized individual.

With respect to Claim 36-39, Ishii meets all the limitation except the limitation disclosed below.

The limitation "creating each individual request from a corresponding multiple certification request recorded in the storage means…" is met by Van Oorschot on column 3, lines 20-38.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Van Oorschot to the system of Ishii so as to allow for the secure creation of keys for the required authorized individual.

The combination of Ishii and Van Oorschot do not disclose the set of keys belonging to a preset list of keys. This is however disclosed by Aziz.

The limitation "...relative to a set of pairs of keys for subjects belonging to a preset list or to a set of pairs of keys for subjects defined by predetermined criteria, as well as to associated model certificates for the set in question" is met by Aziz on column 4, lines 1-21.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Aziz within the combination of Ishii and Van Oorschot so as to allow for the retrieval of an already authorized list of subjects and hence lessens the likelihood for the creation and transmission of keys to an unauthorized individual.

With respect to Claims 40-43, all the limitation is met by the combination of Ishii and Aziz. The limitation "searching in each of the multiple creation and certification requests of the system for all of the subjects in a condition such that a pair of keys must be created" is met by Van Oorschot on column 4, lines 37-47.

It would have been obvious to one of ordinary skill in the art to combine the teachings of Van Oorschot to the combination of Ishii and Aziz so as to allow for the creation and distribution of secure keys.

Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (5768389) in view of Van Oorschot (6370249B1) in further view of Schneier.

The combination of Ishii and Van Oorschot meets all the limitation except for the limitation disclosed below.

The limitation "characterized in that each multiple request comprises an attribute relative to at least one execution date and in that said process consists of including in the search only the multiple requests whose expiration date has arrived" is met by Schneier on page 183-184, section 8.10.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Schneier within the combination of Ishii and Van Oorschot so as to prevent the existence of keys for an extended period of time and hence lessen the likelihood of the keys being compromised as disclosed by Schneier within the same excerpt.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 703-305-7820. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7240 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

***
October 30, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100